LIIKETOIMINNAN RISKIENHALLINNAN JA JATKUVUUDENHALLINNAN SUUNNITELMAT

Keski-Suomen Kuljetus Oy

Johanna Könönen

Opinnäytetyö
Joulukuu 2012

Tietotekniikka
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä KÖNÖNEN, Johanna	Julkaisun laji Opinnäytetyö	Päivämäärä 12.12.2012
	Sivumäärä 43	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
LIIKETOIMINNAN RISKIENHALLINNAN JA JATKUVUUDENHALLINNAN SUUNNITELMA
Case: Keski-Suomen Kuljetus Oy

Koulutusohjelma
Tietotekniikan (Tietoverkkotekniikan) koulutusohjelma

Työn ohjaaja
HAUTAMÄKI, Jari

Toimeksiantaja
Keski-Suomen Kuljetus OY

Tiivistelmä
Opinnäytetyön tarkoituksena oli laatia liiketoiminnan riskienhallinnan ja jatkuvuudenhallinnan suunnitelma Keski-Suomen Kuljetus Oy:lle. Keski-Suomen Kuljetus Oy on kuljetuspalveluja, maarakennusurakointia ja kiviaineskauppaa harjoittava yritys. Erilaisten tietojärjestelmien ja sähköisten järjestelmien lisääntyminen tuo haasteita myös tietoturvallisuuteen ja sen ymmärtämiseen. Tämän takia Keski-Suomen Kuljetus Oy:lle laadittiin myös tietoturvaperiaatteet ja käytänteet.

Opinnäytetyö aloitettiin Huoltovarmuuskeskuksen suorittaman kypsyysanalyysin tulosten pohjalta. Kypsyysanalyysin tarkoituksena on selvittää, kuinka hyvin yritys on varautunut liiketoiminnan häiriötilanteisiin ja määritellä mikä on liiketoiminnan kannalta järkevä tavoitetaso.

Tarvittavan pohjatiedon keräämisen ja lähdemateriaalien tutkimisen jälkeen aloitettiin käytännön työ. Määriteltiin suojeltavat kohteet, suoritettiin riskikartoitus ja tulosten perusteella laadittiin riskienhallinnan ja jatkuvuudenhallinnan suunnitelma.

Opinnäytetyön lopputuloksena syntyi liiketoiminnan riskienhallinnan ja jatkuvuudenhallinnan suunnitelma, joka pitää sisällään tietoturvaperiaatteet ja käytänteet sekä kriisiviestintäohjeen.

Avainsanat (asiasanat)
riskienhallinta, riskianalyysi, jatkuvuudenhallinta, tietoturvaperiaatteet, tietoturvakäytänteet, tietoturva

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Author	Type of publication	Date
KÖNÖNEN, Johanna	Bachelor´s Thesis	12122012
	Pages 43	Language Finnish
		Permission for web publication (X)

Title
MANAGEMENT PLANS FOR BUSINESS RISKS AND CONTINUANCE
Case: Keski-Suomen Kuljetus Ltd.

Degree Programme
Information Technology

Tutor
HAUTAMÄKI, Jari

Assigned by
Keski-Suomen Kuljetus Ltd.

Abstract

The main purpose of this thesis was to draw up management plans for business risks and continuance for Keski-Suomen Kuljetus Ltd. Keski-Suomen Kuljetus Ltd.'s services comprise transport, earthworks and rock material business. The increase in understanding different information and electricity systems presents a challenge for the company, which is why the task was to draw to up also information security principles and information security practices for Keski-Suomen Kuljetus Ltd.

Huoltovarmuuskeskus made a maturity analysis and it was the first step for this thesis. The purpose of the test was to find out how well the company is prepared to meet potential business operation incidents and to determine the reasonable level for the risks.

After examining the source material and collecting the basic data the practical work started. The issues to be protected were determined, the risk analysis was performed and based on the results management plans for business risks and continuance were created.

The final results of this thesis were the created management plans for business risks and continuance. The management plan includes also information security principles and information security practices as well as the instructions for crisis communication.

Keywords
Risk management, continuance management, information security principles, information security practices, information security

Miscellaneous

Sisältö

1 TYÖN LÄHTÖKOHDAT

Tässä opinnäytetyössä käydään yleisellä tasolla läpi liiketoiminnan riskienhallinnan ja liiketoiminnan jatkuvuudenhallinnan suunnitelman eri vaiheita. Työssä laadittiin ko. suunnitelma Keski-Suomen Kuljetus Oy:lle ja työhön sisällytettiin:

- suojeltavien kohteiden määrittely
- riskikartoitus
- tietoturvaperiaatteet ja käytänteet
- kriisiviestintäohje
- jatkuvuus- ja toipumissuunnitelma.

Keski-Suomen Kuljetus Oy on huoltovarmuuskriittinen yritys, mikä tarkoittaa, että kuljetuslogistiikkatoimiala varautuu turvaamaan yhteiskunnan elintärkeät kuljetus- ja logistiikkapalvelut normaalioloissa, vakavissa häiriötilanteissa ja poikkeusoloissa. Keski-Suomen Kuljetus Oy:ssä siirrytään koko ajan yhä enemmän kohti sähköisiä järjestelmiä, ja yhtiöltä puuttuvat tietoturvakäytänteet ja -periaatteet. Tämän opinnäytetyön tarkoitus oli paikata tätä puutetta.

Työ alkoi Huoltovarmuuskeskuksen tekemällä kypsyysanalyysillä. Kypsyysanalyysin tarkoituksena oli selvittää yrityksen kyky varautua mahdollisiin liiketoimintaan kohdistuviin tulevaisuuden häiriötilanteisiin ja määrittelemällä mikä on liiketoiminnan kannalta järkevä tavoitetaso. Seuraavaksi tutkittiin aiheeseen liittyvää lähdemateriaalia ja kerättiin pohjatietoa. Selvitettiin esimerkiksi mitä tarkoitetaan riskien- ja jatkuvuudenhallinnalla sekä tietoturvakäytänteillä ja – periaatteilla.

Keski-Suomen kuljetus Oy on vuonna 1962 perustettu kuljetuspalveluja, maarakennusurakointia ja kiviaineskauppaa harjoittava yritys. Yhtiöllä on viisi aluetoimistoa Keski-Suomessa; Jämsässä, Muuramessa, Jyväskylässä, Saarijärvellä ja Viitasaarella. Toimialue on koko Keski-Suomi. Rahtia yhtiö kuljettaa koko Suomen alueella.

2 LIIKETOIMINNAN RISKIENHALLINTA

Liiketoiminnan riskienhallinnalla tarkoitetaan, että yritys varautuu jo tänään mahdollisiin tulevaisuuden häiriötilanteisiin. Tunnistamalla yritystoimintaan, niin henkilöstöön kuin liiketoimintaankin, kohdistuvia riskejä yritys turvaa liiketoiminnan jatkuvuuden. Jokainen henkilöstön jäsen osallistuu riskienhallintaan oman vastuualueensa osalta, arvioimalla tilanteita, suunnittelemalla ja käytännön teoilla. Mahdollisten riskien tiedostaminen ja ennakointi sekä riskeihin suunnitelmallisesti ja järjestelmällisesti varautuminen, on hyvää riskienhallintaa. Riskienhallinta on jatkuvaa toimintaa.

Riskienhallintasuunnitelma pitää sisällään

- riskien arvioinnin
- tarvittavien toimenpiteiden suunnittelun
- toteutuksen
- seurannan
- korjaavat toimenpiteet.

(Maakuljetuspooli, 2012).

Riskienhallintasuunnitelman ei tarvitse olla monimutkainen, mutta sen tulisi kattaa koko yrityksen toiminta. Tämän vuoksi riskienhallintasuunnitelmasta kannattaa tehdä järkevän kokoinen, jotta se olisi mahdollisimman hyvin hallittavissa. Koska riskienhallinta on jatkuvaa toimintaa, voidaan eri riskien toiminnallisia suunnitelmia lisätä riskienhallintasuunnitelmaan myöhemminkin.

Riskienhallintasuunnitelman laatiminen aloitetaan riskikartoituksella, mistä kerrotaan lisää luvussa 4.

3 SUOJELTAVIEN KOHTEIDEN MÄÄRITTELY

Suojeltavien kohteiden määrittelyllä tarkoitetaan sitä, että yrityksessä pohditaan ja dokumentoidaan liiketoiminnan kannalta tärkeimmät suojeltavat asiat. Sellaisia voivat olla esimerkiksi IT-järjestelmät, fyysiset dokumentit ja liiketoiminta-alueet. Kun suojeltavat asiat on dokumentoitu, niille määritellään tavoitetaso tarvittavan suojan takaamiseksi. Suojeltavia asioita voidaan tunnistaa esimerkiksi uhkaskenaarion avulla. Uhkaskenaarion tarkoitus on kuvata liiketoiminnan tärkeimpien suojeltavien asioiden näkökulmasta konkreettisesti erilaisten uhkien mahdollisia toteutumistapoja (Rosqvist Tony, Tuominen Risto & Sarsama Janne 2006, 10).

Suojeltavat asiat luokitellaan kriittisyyden mukaan eri luokkiin. Liiketoiminnan kannalta tärkeimmät järjestelmät on suojattava ensin. Ne siis merkitään tärkeysjärjestyksen kärkipäähän. Vastaavasti liiketoiminnan kannalta vähemmän tärkeät asiat sijoittuvat luokittelussa alempaan luokkaan. (Maakuljetuspooli, 2012.)

4 RISKIKARTOITUS

Suojeltavien kohteiden määrittelyn jälkeen tehdään riskikartoitus. Riskikartoitus tarkoittaa sitä, että pohditaan, mitä uhkia suojeltaviin asioihin kohdistuu ja dokumentoidaan ne. Uhkien dokumentoinnin jälkeen arvioidaan uhkien merkitys, luokitellaan uhat ja määritellään keinot, joilla uhkia hallitaan.

Riskien arvioinnin tulisi olla liiketoiminnassa jokapäiväistä toimintaa, koska ympäröivässä maailmassa tapahtuu koko ajan muutoksia.

Riskikartoitus tulisi toteuttaa säännöllisesti ja systemaattisesti. Kartoituksen toteutukseen osallistuvat ydintoimintojen tuloksista vastaavat ja ydintoimintoja tukevista toiminnoista vastaavat henkilöt. (Maakuljetuspooli, 2012).

Riskikartoituksen tehtävä on

- tunnistaa toiminnan uhat (sisäisen ja ulkoisen toiminnan häiriötilanteet ja vaaratekijät)
- arvioida riskit eli tunnistettujen uhkien todennäköisyys ja niistä aiheutuvien seurausten vakavuus
- luokitella riskit
- suunnitella ja ehdottaa tarvittavat riskienhallintakeinot ja -toimenpiteet, joilla riski poistetaan, estetään, rajataan, siirretään tai hyväksytään
- raportoida päätettäväksi riskit ja ehdotetut riskienhallintakeinot ja -toimenpiteet
- päättää riskienhallintakeinojen ja -toimenpiteiden toteutus
- seurata päätettyjen toimenpiteiden toteutusta
- suorittaa riskianalyysi uudestaan

Huoltovarmuuskeskuksen laatima ohje riskikartoituksesta sisältää viisi vaihetta:

1. Suojeltavan kohteen täsmentäminen
2. Uhkien tunnistaminen ja dokumentointi
3. Uhkan todennäköisyyden ja vaikutuksen määrittely
4. Korjaavien toimenpiteiden määrittely
5. Raportointi

Riskikartoituksessa on hyvä käyttää apuna riskikartoituslomaketta. (Katso kuvio 1)

Riskianalyysin kohde:

Yksikkö:	**Vastuujohtaja:**	**sivu 1/2**
Kriittinen toiminto/kohde:	**Osallistujat:**	**Päivämäärä:**

Osa-alue	**Uhka**	**Toden-näköisyys**	**Vaiku-tus**	**Tulos**	**Korjaavat toimenpiteet**	**Toden-näköisyys**	**Vaiku-tus**	**Tulos**
Johtaminen								
Toimintaperiaatteet								
Henkilöstö								

KUVIO 1 Riskikartoituslomake (Maakuljetuspooli, 2012)

Vaihe 1. Suojeltavan kohteen määrittäminen

Rajataan yrityksen toiminto tai osasto suojeltavaksi kohteeksi, kuvion 1 yläosa. Määritellään toimintoon liittyvät osa-alueet, joihin kohdistuvia uhkia pyritään tunnistamaan. Kuviossa 1 tällaisia toimintoja ovat johtaminen, toimintaperiaatteet ja henkilöstö.

Vaihe 2. Uhkien tunnistaminen ja dokumentointi

Kunkin osa-alueen uhat tunnistetaan ja kirjataan kuvion 1 kohtaan uhka. Uhkien tunnistaminen edellyttää liiketoiminnan ja sitä uhkaavien yllättävien tilanteiden tuntemista ja mahdollisten tilanteiden ideointikykyä. Toimintaa häiritseviä tilanteita aiheuttavat esimerkiksi

- luonnonilmiöt, kuten myrskyt ja ukkoset
- ihmisten toiminta, vahinko tai tahallinen

- toimintaympäristöstä aiheutuvat tilanteet, sähkökatkot tai kemikaalivuodot.

Vaihe 3. Uhkan todennäköisyyden, vaikutuksen määrittely

Uhkien todennäköisyys voidaan arvioida taulukon 1 avulla ja tulokset kirjataan kuvion 1 kohtaan todennäköisyys.

TAULUKKO 1 Todennäköisyystasot (Maakuljetuspooli, 2012)

Todennäköisyys	Todennäköisyyden määrittely
1	äärimmäisen harvinainen riski (ei 5 vuodessa)
2	harvinainen (4v -5 v)
3	melko harvinainen (2 v - 4 v)
4	melko todennäköinen (6 kk -2 v)
5	erittäin todennäköinen riski (6 kk)
6	varma (1 kk)

Uhkien vaikutus arvioidaan taulukon 2 avulla ja kirjataan kuvion 1 kohtaan vaikutus.

TAULUKKO 2 Vaikutustasot (Maakuljetuspooli, 2012)

Vaikutus	Vaikutuksen määrittely
1	mitätön vaikutus
2	lievä
3	haitallinen
4	merkittävä / tuntuva vaikutus
5	suuri / vakava vaikutus
6	tuhoisa vaikutus, katastrofi

Uhkien riskiluku saadaan riskitasotaulukosta (katso taulukko 3), uhkan todennäköisyyden ja vaikutuksen kohdalta tai uhkan todennäköisyyden ja vaikutuksen tulona. Tämä luku kirjataan kuvion 1 kohtaan tulos.

TAULUKKO 3 Riskitaso (Maakuljetuspooli, 2012)

		Vaikutus					
Todennäköisyys		**Matala**		**Keskisuuri**		**Korkea**	
		1	**2**	**3**	**4**	**5**	**6**
Matala	**1**	1	2	3	4	5	6
	2	2	4	6	8	10	12
Keskisuuri	**3**	3	6	9	12	15	18
	4	4	8	12	16	20	24
Korkea	**5**	5	10	15	20	25	30
	6	6	12	18	24	30	36

Riskiskaala: Erittäin korkea 25-36, korkea 15-24, keskisuuri 5-12, matala 1-4.

Vaihe 4. Korjaavien toimenpiteiden määrittely

Riskitason (erittäin korkea, korkea, keskisuuri ja matala) mukaan arvioidaan taulukosta 4 toteutettavat toimenpiteet, joihin ylimmän johdon ja toiminnon omistajan täytyy ryhtyä kullakin riskitasolla.

TAULUKKO 4 Riskiasteikko määrittelee toiminnot eri riskiluokille (Maakuljetuspooli, 2012)

Riskiluokka		**Riskiasteikko: Suositeltavat riskienhallinnan toimenpiteet**
Matala	**1-4**	Ei edellytä riskienhallintakeinojen toteuttamista.
Keski-suuri	**5-12**	Kohtalainen tarve toteuttaa uusia riskienhallinnan toimenpiteitä / keinoja. Aikataulu sovittavissa.
Korkea	**15-24**	Merkittävä tarve toteuttaa mahdollisimman nopeasti uusia riskienhallinnan toimenpiteitä / keinoja.
Erittäin korkea	**25-36**	Erittäin merkittävä tarve toteuttaa välittömästi riskienhallinnan toimenpiteitä / keinoja.

Kunkin uusia riskienhallinnan toimenpiteitä tai keinoja edellyttävän riskin kohdalla arvioidaan mitä pitää tehdä, jotta riskin riskiluokka pienenee hyväksyttävälle tasolle. Riskienhallintakeinoina ovat riskin hyväksyminen, ehkäisy, rajoittaminen, suunnittelu ja siirtäminen. Riskien käsittelyn vaihtoehdot ja toimenpiteet ovat taulukossa 5. Tarvittavat toimenpiteet ja keinot voidaan dokumentoida kuvion 2 kehittämissuunnitelmalomakkeelle.

TAULUKKO 5 Riskien käsittelyn vaihtoehdot ja toimenpiteet (Maakuljetuspooli, 2012)

Riskin käsittely	Toimenpiteet
hyväksyminen	Toiminnan jatkaminen ja riskin hyväksyminen. Pienennetään riskiä sopivin keinoin, esimerkiksi suojavarustuksella.
ehkäisy	Poistetaan riskin syy tai seuraus.
rajoittaminen	Uhkan vaikutusta pienennetään rajoittamalla riskiä.
suunnittelu	Riskiä hallitaan hyvällä suunnittelulla, esimerkiksi laatimalla riskienhallintasuunnitelma ja ylläpidetään sitä.
siirtäminen	Riskin vaikutusta pienennetään siirtämällä siitä osa toisen tai kolmannen osapuolen toimijalle, esimerkiksi ottamalla vakuutus.

Riskikartoituksen kohde:

Yksikkö:	**Vastuujohtaja:**	**sivu 1/1**
Kriittinen toiminto/kohde:	**Osallistujat:**	**Päivämäärä:**

Toimenpide	Vastuuhenkilö	Ajoitus	Kustannus	Tulos

KUVIO 2 Kehittämissuunnitelma (Maakuljetuspooli, 2012)

Vaihe 5. Raportointi

> Kun riskien arviointi on suoritettu ja suositeltavat riskienhallinnan toimenpiteet ja keinot on määritelty, tulokset dokumentoidaan riskiraportiksi.
>
> Raportti ohjaa johtamista ja auttaa ylintä johtoa ja organisaation toimintojen omistajia tekemään päätöksiä toimintapolitiikoista, toimintamalleista, budjetista ja toimintajärjestelmän ja johtamisjärjestelmän muutoksista.
>
> Raportti kuvaa systemaattista ja analyyttista lähestymistä riskien arviointiin, jotta ylin johto ymmärtää, että riskit ja niihin hallintaan kohdennetut resurssit vähentävät potentiaalisia menetyksiä.

Riskikartoitus toteutetaan säännöllisesti ja siinä otetaan huomioon aina edellisen kartoituksen riskit, havainnot ja toimenpide-ehdotukset (Maakuljetuspooli, 2012).

5 TIETOTURVAPOLITIIKKA

Tietoturvapolitiikka on ensimmäinen asia, joka tehdään riskikartoituksesta paljastuvien epäkohtien korjaamiseksi. Yritysjohto laatii ja allekirjoittaa tietoturvapolitiikan. Tietoturvapolitiikassa määritellään tietoturvan kohteet, periaatteet sekä määritellään vastuut ja koulutustarpeet. Tietoturvapolitiikassa on otettava huomioon lakien ja sopimusten toiminnalle asettamat vaatimukset. Tietoturvapolitiikkaan kirjataan myös tietoturvan laiminlyöntitapausten käsittely. Tietoturvapolitiikan tarkoitus on osoittaa yritysjohdon sitoutuneisuus tähän prosessiin, sekä motivoida ja rohkaista henkilöstöä tietoturvallisempiin toimintatapoihin. (Laaksonen Mika, Nevasalo Terho & Tomula Karri 2006, 146.)

Tietoturvapolitiikka on omalle yritykselle tehty dokumentti, ei Internetistä löytyvä toisen yrityksen tietoturvapolitiikan kopio. Tietoturvapolitiikka otetaan käyttöön koko yrityksessä. Yrityskulttuurista ja työntekijöiden tietoturvan osaamisen määrästä riippuu tietoturvapolitiikan ja toimintaohjeiden noudattamisen ja

valvonnan taso. Jatkuva koulutus ja tietoturvatietoisuuden lisääminen ovat välttämättömiä edellytyksiä hyvän tietoturvatason saavuttamiseksi (Mäkinen Riitta 2003, 3).

6 LIIKETOIMINNAN JATKUVUUDENHALLINTA

Useista eri toimijoista muodostuvissa verkostoissa tuotetaan tämän päivän palvelut ja tuotteet. Näin ollen yhteiskunnan huoltovarmuuteen vaikuttaa koko verkoston toimintakyvyn ylläpitäminen. Verkoston toimintakykyä parannetaan verkostoon kuuluvan organisaation omaa toimintakykyä kehittämällä. (Huoltovarmuuskeskus, 2012.)

Yrityksen toimintaa uhkaavien häiriötilanteiden hallintaan suunnitellut ja toteutetut järjestelyt sekä johtamismallit ovat niitä toimenpiteitä joita kutsutaan jatkuvuudenhallinnaksi. Jatkuvuudenhallinnan menettelytavat takaavat osaltaan kansalaisille, yrityksille ja organisaatioille suunnattujen palveluiden saatavuuden häiriötilanteissa ja poikkeusoloissa. (Huoltovarmuuskeskus, 2012.)

Jatkuvuudenhallinta on organisaatioille työkalu, jonka avulle ne voivat

- havaita liiketoimintaansa kohdistuvat mahdolliset riskit ja häiriötilanteet,
- kehittää häiriötilanteiden varalle toimintamallit,
- varmistua siitä, miten hyvin tärkeimmät sidosryhmät ovat varautuneet mahdollisiin häiriötilanteisiin.

Jatkuvuudenhallinnan järjestelmällisen kehittämisen tarkoitus on minimoida häiriötilanteista toipumiseen kuluvaa aikaa, koska toimintakatkoksista aiheutuu aina kustannuksia. Mikäli yrityksen vastuuhenkilöillä on tarvittavat keinot ja taidot toimia häiriötilanteissa, on toipuminen häiriötilanteista huomattavasti nopeampaa. Yrityksen järjestelmällinen ja suunnitelmallinen toiminta normaali oloissa, antaa yrityksen toimintakyvystä häiriötilanteissa luotettavamman ja uskottavamman kuvan. (Huoltovarmuuskeskus, 2012.)

7 TIETOTURVA

Tietoturva tarkoittaa informaation turvaamista. Kaikilla yrityksillä on liiketoiminnan kannalta tärkeitä suojeltavia tietoja esimerkiksi liikesalaisuudet ja henkilötiedot. Tietoturvasta noin 20% on niin sanottua teknistä turvaamista kuten, palomuurilaitteistojen ja virustorjuntaohjelmistojen käyttöä. Loput 80% on hallinnollista tietoturvaa kuten, kouluttamista ja toimintatapojen ohjeistamista. (Tietoturvatietoa suomeksi, 2012a.)

Tietoturva koostuu viidestä tavoitteesta: tiedon luottamuksellisuus, eheys, saatavuus, kiistämättömyys ja todentaminen.

Luottamuksellisuudella tarkoitetaan sitä, että tieto on vain niiden henkilöiden käytettävissä, joille se kuuluu.

Eheydellä pyritään siihen, että tieto säilyy muuttumattomana tiedonsiirron ajan.

Saatavuudella tarkoitetaan sitä, että tieto on käytettävissä silloin kun sitä tarvitaan.

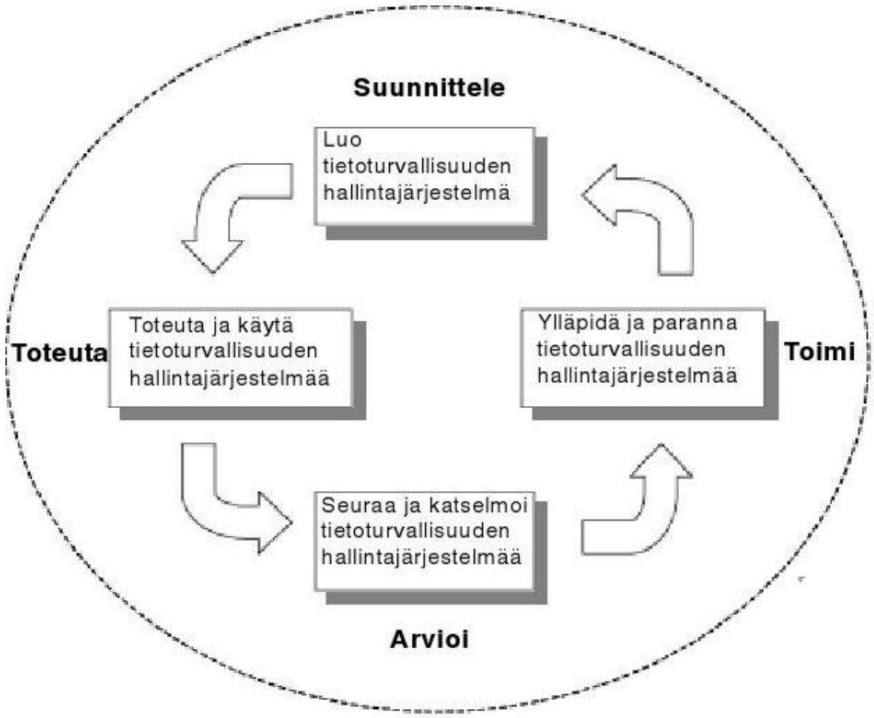
Kiistämättömyydellä tarkoitetaan tapahtuneen todistamista jälkeenpäin. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa jälkeenpäin. Tietojärjestelmien tapahtumat voidaan tallettaa lokitiedostoihin, joista käy kiistämättömästi ilmi käyttäjien tapahtumat tiettyinä kellonaikoina.

Todentaminen tarkoittaa sitä, että henkilö todistaa esimerkiksi tietojärjestelmälle olevansa juuri ne valtuudet omaava henkilö. Tyypillisimmillään todennus tapahtuu käyttäjätunnuksella ja salasanalla.

Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuus hallintajärjestelmä on samankaltainen johtamisjärjestelmä kuin esimerkiksi laatujohtamisjärjestelmä. Tietoturvallisuuden hallintajärjestelmän kehittämisessä voidaan käyttää apuna niin sanottua PDCA-mallia (Plan-Do-Check-Act) eli suomenkielisenä Suunnittele-Toteuta-Arvioi-Toimi. PDCA-mallin avainkohdat on esitetty kuviossa 3. Ensimmäisessä vaiheessa

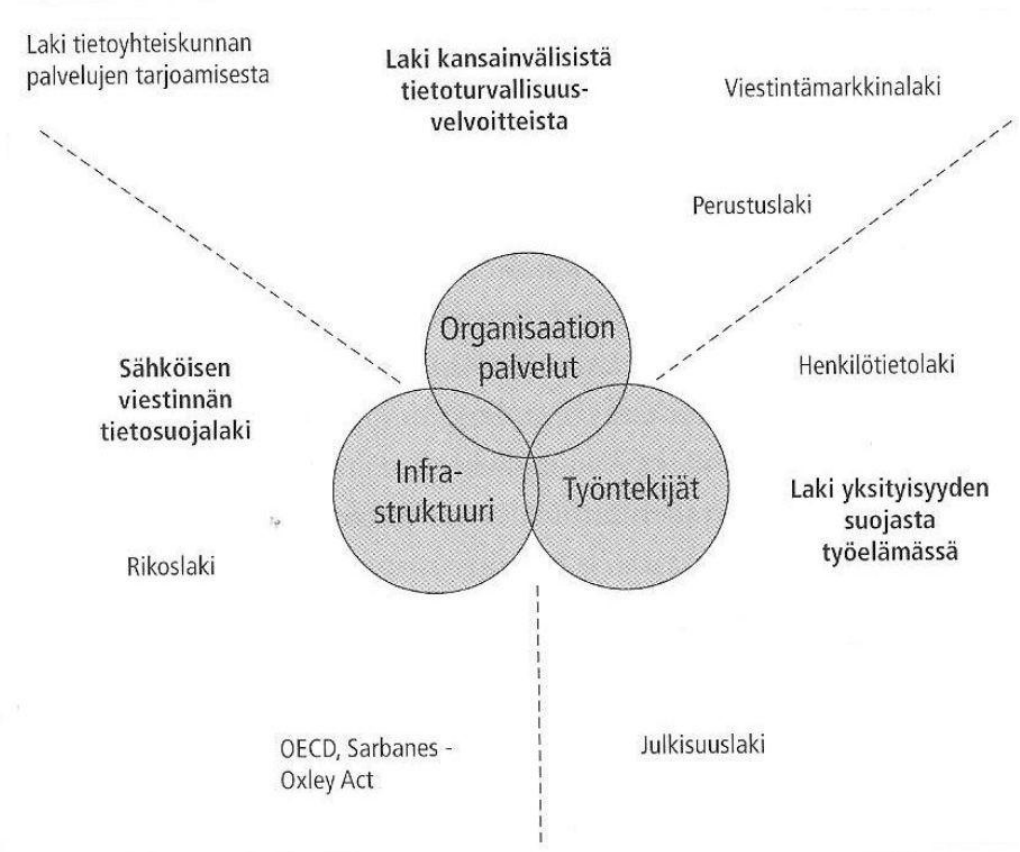
eli suunnitteluvaiheessa määritellään suojattavat kohteet, mietitään millainen tietoturvan taso on yrityksen liiketoiminnan kannalta sopiva taso ja viimeiseksi laaditaan tietoturvallisuuden hallintajärjestelmä. Tietoturvallisuuden hallintajärjestelmän toteutuksen jälkeen alkaa työn arviointi ja oikeaan suuntaan kehittäminen. Prosessi on jatkuvaa toimintaa ja tilanteiden muuttuessa tietoturvallisuuden hallintajärjestelmän PDCA-mallin mukaiset vaiheet alkavat alusta (ISO/IEC 27001:fi 2006, 8).



KUVIO 3 Tietoturvallisuuden hallintajärjestelmän PDCA-mallin mukaiset vaiheet (ISO/IEC 27001:fi 2006, 8)

7.1 Lainsäädännön vaikutukset

Lainsäädäntö ohjaa yrityksen liiketoimintaa. Myös tietoturvaa suunniteltaessa, toteuttaessa ja kehittäessä on otettava huomioon laissa määrätyt asiat. Kuvio 4 helpottaa ymmärtämään sen miten eri lainsäädännöt käsittelevät tietoturvaa.



KUVIO 4 Tietoturvaa käsittelevät lait (Laaksonen Mika, Nevasalo Terho & Tomula Karri 2006, 23)

Yrityksen toiminta on jaettu kolmeen kategoriaan: palveluihin, infrastruktuuriin ja työntekijöihin. Samaten lait on jaettu eri kategorioihin, jotta olisi helpompi hahmottaa, mikä laki koskee yrityksen mitäkin toimintaa. Kuvio on viitteellinen. Eri kategorioiden välillä on päällekkäisyyksiä, mutta kuvasta voi hahmottaa esimerkiksi, että työntekijöiden omaan tietoturvaan vaikuttavia lakeja ovat henkilötietolaki ja laki yksityisyyden suojasta työelämässä. Luottamuksellisten henkilöstöä koskevien tietojen käsittely IT-järjestelmissä on määritelty sähköisen viestinnän tietosuojalaissa, joka on osa infrastruktuuri-osiota (Finlex, 2004).

Tietoturvaan vaikuttaa valtava määrä lakeja, kuten kuviosta 4 sen voi havaita. Yrityksen näkökulmasta asian hallintaa hankaloittaa vielä se, että säädökset on jaettu useisiin eri lakeihin. Erillistä tietoturvalakia Suomeen ei ole vielä säädetty. Viranomaisilta halutaan enemmän ohjeistusta tietoturvan suojamekanismien, valvonnan ja vaatimusten lainmukaiseen toteuttamiseen. (Tietoturvatietoa suomeksi, 2012b.)

7.2 Standardit ja sertifiointi

Tietoturvallisuuden hallintajärjestelmän voi myös sertifioida, mikäli yritys katsoo sellaisen tarpeelliseksi. International Organization for Standardization (ISO) on kansainvälinen organisaatio, joka määrittelee sertifioinnissa vaadittavat kriteerit. Vaatimukset ovat kuvattu ISO/IEC 27001-standardissa.

Viralliset standardit ovat maksullisia, mutta saatavilla on myös ilmaisia vaihtoehtoja. Valtiohallinnon VAHTI-työryhmä tarjoaa tietoturvallisuuteen liittyviä ohjeistuksia ja suosituksia Suomen kielellä (Valtiovarainministeriö, 2012).

7.3 Tietoturvaperiaatteet -ja käytännöt

Yrityksen on selvitettävä suojeltavat asiat ja niitä uhkaavat riskit ennen tietoturvaperiaatteiden ja -käytäntöjen kirjaamista. Lainsäädännön ja mahdollisten muiden sopimusvelvoitteiden vaatimukset on myös selvitettävä ennen tietoturvakäytänteiden luomista. Yrityksen koosta ja toimialasta riippuen tietoturvatarpeet vaihtelevat teknisten ja fyysisten vaatimusten osalta.

Tietoturvatietoa suomeksi - verkkosivuston mukaan tietoturva koostuu kahdeksasta osa-alueesta:

- Hallinnollinen tietoturva - Johtaminen ja hallinnointi sekä tietoturvapolitiikka
- Fyysinen tietoturva - Toimitilojen ja laitteiden fyysinen suojaaminen
- Laitteistoturvallisuus – Teknisten laitteiden suojaaminen
- Ohjelmistoturvallisuus – Ohjelmistoihin ja lisensseihin liittyvät tietoturvaasiat
- Tietoaineiston turvallisuus – Tietojen suojaaminen, esimerkiksi varmuuskopioiden käsittely
- Tietoliikenneturvallisuus – Sähköisen tiedon siirtämiseen liittyvät asiat

- Henkilöstöturvallisuus – Henkilöstöön ja sidosryhmiin liittyvät tietoturva-asiat

- Käyttöturvallisuus – Päivittäisiin toimintoihin liittyvät asiat.

(Tietoturvatietoa suomeksi, 2012c.)

7.3.1 Hallinnollinen tietoturva

Kaikki liiketoiminnan prosessit tarvitsevat johtamista ja kehittämistä, niin myös tietoturvallisuus. Hallinnollinen tietoturva sisältää menettelytavat tietoturvan osa-alueiden ohjaamiseen, esimerkiksi henkilöstön organisointiin, dokumentaatioon, yleisiin linjauksiin ja tietoturvapolitiikkaan (Hakala ym. 2006, 10–11).

ISO/IEC 27001-standardin mukaan merkittävimmät hallinnollisessa tietoturvassa huomioitavat ja dokumentoitavat asiat on listattu taulukkoon 6.

Tietoturvan johtaminen on laaja käsite, mutta tärkeintä on huomioida, että toimintatavat ovat lainsäädännöllisesti oikein.

TAULUKKO 6 Hallinnollisessa tietoturvassa huomioitavia ja dokumentoitavia asioita (ISO/IEC 27001:fi 2006, 32–34) (Laakso Matti 2010, 39)

Aihe	Selite
Tämän hetken tilanteen selvittely	Selvitetään tietoturvallisuuden tämän hetken taso ja kehityskohteet. Selvitetään lainsäädännön vaikutukset. Määritellään järkevä tavoitetaso.
Riskienhallinta	Kartoitetaan sisäiset ja ulkoiset riskit sekä analysoidaan ne.
Yritysjohdon sitoutuminen	Yritysjohdon tulee sitoutua ja olla esimerkkinä tietoturvatyössä sekä järjestää tietoturvatyöhön tarvittavat resurssit.

Tietoturvapolitiikka	Tietoturvapolitiikka ohjaa yrityksen toimintaa.
Vastuualueet, organisointi ja viestintä	Vastuuhenkilöiden nimeäminen. Viestintä ja raportointikäytännöistä sopiminen.
Tietoturvaohjelman laatiminen	Sisältää tarpeeksi kattavan ohjeistuksen ja koulutuksen tarjoamisen työntekijöille. Tietoturvaohjelman tavoitteena on tietoturvatietouden lisääminen ja ohjeiden kehittäminen.
Sopimukset	Henkilöstöön ja sidosryhmiin liittyvissä sopimuksissa on mainittava tietoturva-asiat.
Suunnitelmat	Laaditaan jatkuvuussuunnitelma, toipumissuunnitelma ja tietoturvankehittämissuunnitelma ja ylläpidetään niitä.

7.3.2 Fyysinen tietoturva

Fyysinen tietoturva tarkoittaa sitä, että yrityksen toimitilat ja laitteet suojataan esimerkiksi tulipalon, vesivahingon tai varkauden varalta. Fyysinen tietoturva on tärkeä osa kokonaisvaltaisen tietoturvan hallintaa. Muita fyysisessä tietoturvassa huomioon otettavia asioita on taulukossa 7.

TAULUKKO 7 Fyysisessä tietoturvassa huomioitavia ja dokumentoitavia asioita (ISO/IEC 27001:fi 2006, 38) (Laakso Matti 2010, 40)

Aihe	Selite
Turva-alueet	Määritellään toimitilojen turva-alueet ja luokitellaan ne tärkeysjärjestykseen.
Suojaaminen	Otetaan käyttöön eri alueiden suojatoimenpiteet. Esimerkiksi kulunvalvonta, murtohälyttimet tai paloturvallisuuteen vaikuttavat tekijät. Lisäksi dokumentoidaan ne.
Kouluttaminen	Ohjeiden laatiminen laitteiden ja tapahtumien hallintaan. Varmistetaan, että henkilöstöllä on riittävä osaaminen fyysisen tietoturvan suojaamisessa.
Riskitekijät	IT-tiloissa olevat mahdolliset riskitekijät, kuten esimerkiksi vesipisteet, on otettava huomioon tietoturvallisuuden näkökulmasta.

Yrityksen koko, toimiala ja henkilökunnan määrä vaikuttavat siihen, millaisia suojakeinoja toimitilat vaativat. Tietotekniikka-alalla toimivan yrityksen fyysisen tietoturvan on oltava kunnossa, kun taas muulla toimialalla toimivan yrityksen suojaamiset kohdentuvat muualle. Toimitilat voidaan jakaa tärkeyden mukaan erilaisiin turva-alueisiin, jolloin turvatoimet kohdennetaan ensisijaisesti tärkeimpiin alueisiin.

7.3.3 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan yrityksen laitteiden, esimerkiksi kannettavien tietokoneiden, tulostimien, palvelimien ja matkapuhelimien suojaamista. Ihan ensimmäiseksi kannattaa inventoida yrityksessä olevat laitteet ja dokumentoida ne. Laitteet on syytä myös merkitä fyysisesti. Tietoturvaan vaikuttaa myös laitteiden sijainti. Esimerkiksi tietokoneita ei kannata sijoittaa poistumisteiden läheisyyteen, koska siitä ne voidaan helposti kantaa ulos. Odottamattomilta ongelmilta vältytään usein myös silloin kun pidetään laitteet toimintakuntoisina. Palvelimen rikkoutuminen yllättäen aiheuttaa paljon ylimääräistä työtä ja kustannuksia. Varmistamalla jatkuva sähkönsyöttö ja ulkoisilta uhkatekijöiltä suojautuminen vähentää palvelimen rikkoutumisriskiä. Ulkoisia uhkatekijöitä ovat esimerkiksi vedestä ja lämpötilojen vaihteluista aiheutuvat ongelmat.

ISO/IEC 27001-standardin mukaan tärkeimpiä laitteistoturvallisuudessa huomioitavia ja dokumentoitavia asioita on lueteltu taulukossa 8.

TAULUKKO 8 Laitteistoturvallisuudessa huomioitavia ja dokumentoitavia asioita (ISO/IEC 27001:fi 2006, 38–40) (Laakso Matti 2010, 41)

Aihe	Selite
Koneiden ja laitteiden inventaario	Tunnistetaan, dokumentoidaan ja merkitään fyysiset laitteet.
Laitteistopolitiikka	Laitteistopolitiikka määrittää, saako yrityksen tiloissa käyttää esimerkiksi omaa tietokonetta. Eli mitä laitteita yrityksen tiloissa saa käyttää ja mitä laitteita ei saa käyttää.

Laitteistodokumentaatio	Laitteistodokumentaatio sisältää laitteisiin liittyvät ominaisuudet, resurssit, käyttöoikeudet ja ohjeet. Laitteistodokumentaatio sisältää myös laitteisiin tehdyt muutokset.
Yleinen suojaus	Kuvataan suojaustoimenpiteet vesi-, tuli- ja sähkövahinkojen sekä varkauksien estämiseksi
Käyttöoikeudet	Dokumentoidaan laitteiden käyttöoikeuksien tekninen ja hallinnollinen toteuttaminen.
Sopimukset	Dokumentoidaan ja laaditaan huolto- ja ylläpitosopimukset.
Ohjeistaminen	Koulutetaan ja ohjeistetaan laitteiden käyttö.
Vanhojen laitteiden käytöstä poistaminen	Dokumentoidaan toimintaohjeet käytöstä poistettaville laitteille. Esimerkiksi miten vanhat kannettavat tietokoneet tulee hävittää.

Laitteistopolitiikka

Yritysjohdon laatimaa dokumenttia siitä mitä laitteita yrityksessä saa käyttää ja mitä ei saa käyttää kutsutaan laitteistopolitiikaksi. Dokumenttiin kirjataan esimerkiksi säännöt omien tietokoneiden ja tallennusvälineiden käytöstä. Mikäli työpaikka antaa työntekijälle tietokoneen, ei ole tarvetta tuoda yrityksen tiloihin omaa tietokonetta. Ylimääräiset laitteet ovat aina riski tietoturvalle, esimerkiksi virukset ja haittaohjelmat voivat päästä yrityksen verkkoon vieraista laitteista.

Laitteistodokumentaatio

Laitteistodokumentaatio laaditaan helpottamaan tietokoneiden ja muiden laitteiden ylläpitoa. Laitteistodokumentaatioon kirjataan

- koneiden ominaisuudet
- komponentit
- asennetut ohjelmistot
- huoltosopimukset
- ja muut tarvittavat asiat.

Mikäli yrityksessä on paljon samanlaisia tietoteknisiä laitteita, kannattaa ne merkitä, esimerkiksi tarralapuilla, tunnistamisen helpottamiseksi (Miettinen Juha 1999, 224).

7.3.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan tietojärjestelmissä käytettävien ohjelmien ja lisenssien hallintaa. Tietoturvallisuuden kannalta lisenssien hallinta ei kuulosta tärkeältä, mutta se voi johtaa vakaviin tietoturvaloukkauksiin. Mikäli ohjelman lisenssin voimassaolo lakkaa, saattaa itse ohjelmakin lakata toimimasta. Jos kyseessä on esimerkiksi virustentorjuntaohjelma, voivat seuraukset olla ikäviä. Henkilökunnalle on myös syytä ohjeistaa mitä ohjelmia heillä on lupa käyttää työkoneillaan.

Ohjelmistoturvallisuuden olennaisin osa on järjestelmien luvattoman käytön estäminen. Käyttäjän todentaminen, henkilökohtaisten tunnusten ja salasanan avulla, lienee yleisin tapa estää järjestelmien luvaton käyttö. Muitakin tapoja on, esimerkiksi järjestelmän käytön voi estää käyttäjän sijainnin perusteella. Tai jotkin ohjelmistot voidaan rajoittaa toimimaan ainoastaan yrityksen lähiverkosta.

Tietoturvallisuuden kannalta on tärkeää myös se, että yrityksessä on käytössä laadukkaita ohjelmia. Luvattoman käytön esto salasanoilla on turhaa, jos käyt-

täjä pystyy ohittamaan todennusmekanismit. Hyvä ohjelmisto mahdollistaa tapahtumamerkintöjen ja lokimerkintöjen kirjaamisen muistiin. Lokimerkinnät ovat erittäin hyödyllisiä ongelmatilanteiden selvittämisessä. Loki- ja tapahtumamerkinnöistä selviää, kuka käyttäjä on ollut kirjautuneena järjestelmään tiettynä ajankohtana ja miltä koneelta kirjautuminen on tehty. Palvelimet voidaan konfiguroida siten, että ne tallentavat kaiken normaalista poikkeavan toiminnan ja lähettävät siitä tiedon ylläpitäjälle. Näin järjestelmistä vastaavat henkilöt saavat ongelmista heti tiedon. (Miettinen Juha 2002, 169.)

Ihan samalla tavalla kuin laitteisiin myös ohjelmistoihin tulee vikoja, esimerkiksi ohjelmistopäivityksen yhteydessä. Tällaiset viat saattavat pahimmillaan estää ohjelmiston käytön. Ylläpito- ja huoltosopimukset ovat hyvä tapa siirtää vastuuta muille osapuolille. Ohjelmistokorjauksia voi tehdä itse, jos ohjelmiston käyttöoikeudet sen sallivat ja yrityksen tietotaito riittää. Ohjelmistovikojen varalle paras suojautumiskeino on toimiva varmuuskopiointi. Mikäli varmuuskopiointi on hoidettu asianmukaisesti, tietojen palauttaminen on suhteellisen pieni vaiva. Varmuuskopioinnista on hyötyä myös silloin, jos yrityksen tietojärjestelmän lamauttaa haittaohjelma. Uusimmilta uhilta eivät parhaimmatkaan virustorjuntaohjelmat aina suojaa. Mikäli yritys joutuu tällaiseen tilanteeseen, saattaa olla edessä koko järjestelmän uudelleen asentaminen.

ISO/IEC 27001-standardin mukaan tärkeimpiä ohjelmistoturvallisuudessa huomioitavia ja dokumentoitavia asioita on lueteltu taulukossa 9.

TAULUKKO 9 Ohjelmistoturvallisuudessa huomioitavia ja dokumentoitavia asioita (ISO/IEC 27001:fi 2006, 29–31, 48–62) (Laakso Matti 2010, 42)

Aihe	Selite
Ohjelmistojen inventaario	Dokumentoidaan yrityksessä käytössä olevat ohjelmistot sekä niiden versiot ja lisenssit. Nimetään ohjelmistoille vastuuhenkilö.

Ohjelmistopolitiikka	Ohjelmistopolitiikka määrittää, mitä ohjelmistoja yrityksen tiloissa saa käyttää ja mitä ei.
Ohjelmistodokumentaatio	Ohjelmistodokumentaatio sisältää ohjelmistoihin liittyvät ominaisuudet, resurssit, käyttöoikeudet ja ohjeet. Ohjelmistodokumentaatio sisältää myös ohjelmistoihin tehdyt muutokset.
Haittaohjelmilta suojautuminen	Dokumentoidaan keinot joilla suojaudutaan haittaohjelmilta, kuten esimerkiksi viruksilta.
Kouluttaminen	Ohjeistetaan henkilöstöä siitä, miten ohjelmistoja käytetään turvallisesti, päivitysten asentamisen tärkeydestä ja tärkeiden tietojen salaamisesta.
Järjestelmien kuvaukset	Dokumentoidaan esimerkiksi palvelinympäristön tietoturvan lisäämiseksi tehdyt asetusmuutokset. Laaditaan ohjeistus ylläpitäjille.
Varmuuskopiointi	Dokumentoidaan ja ohjeistetaan varmuuskopiointikäytännöt. Tiedotetaan henkilöstölle tarvittaessa.
Sopimukset	Ohjelmistoihin liittyvät tukisopimukset ja avunpyyntöperiaatteet dokumentoidaan.

Ohjelmistopolitiikka

Ohjelmistopolitiikassa kerrotaan, mitkä ohjelmat yrityksessä ovat sallittuja ja mitkä kiellettyjä. Kielletyt ohjelmistot on hyvä perustella esimerkkien avulla, jotta henkilökunta ymmärtää kiellon.

Ohjelmistodokumentaatio

Ohjelmistodokumentaatiosta käy ilmi ohjelmistojen ominaisuudet, resurssit, käyttöoikeudet, käyttöohjeet. Ohjelmistodokumentaatiosta selviää myös ohjelmistoihin tehdyt muutokset.

7.3.5 Tietoaineiston turvallisuus

Tietoaineiston turvallisuudella tarkoitetaan tietojen esimerkiksi henkilötietojen suojaamista. Tietoaineiston turvaaminen aloitetaan tiedon tunnistamisella ja luokittelulla. Lainsäädännön määräykset on muistettava ottaa huomioon, esimerkiksi henkilötietojen käsittelyssä. Yrityksen on päätettävä, miten tiedot luokitellaan. Yksi tapa on jakaa informaatio salaisiin ja julkisiin dokumentteihin. Mikäli tällainen luokittelu on liian karkea, voidaan tiedot jakaa myös sisäisiin ja ulkoisiin, luottamuksellisiin ja salaisiin kategorioihin. Muitakin tapoja toki on. (Raggad Bel 2010, 6-8.)

Tietoaineiston luokittelun jälkeen yrityksen tulee määrittää toimintatavat tietojen säilyttämiselle, varmuuskopioinnille ja hävittämiselle. Toimintatavat on määriteltävä myös varmuuskopioiden säilyttämiselle ja hävittämiselle. Varmuuskopioinnissa on muistettava myös tiedon fyysinen turvallisuus. Esimerkiksi ulkoisille tallennusvälineille tallennetut tiedot on suojattava asianmukaisesti.

Tietoaineiston hävittäminen on tapahduttava siten, ettei tietoa voida enää hävittämisen jälkeen palauttaa. Paperisen tiedon hävittäminen voidaan tehdä paperisilppureita käyttäen tai polttamalla. Sähköisten tietojen hävittämisessä on hyvä muistaa, että pelkkä tiedoston poistaminen muistitikulta, kovalevyltä tai muulta vastaavalta tallennusmedialta ei ole riittävä toimenpide. Sähköisen tiedon hävittämiseen on useita vaihtoehtoja. Tallennusmedian voi hävittää esimerkiksi tuhoamalla sen fyysisesti tai ylikirjoittaa se asiaan soveltuvalla

sovelluksella. Mikäli tiedosta halutaan lopullisesti eroon, on muistettava hävittää myös varmuuskopiot. Jos sähköisen tiedon hävittämistä ei tehdä asianmukaisesti, saattaa arkaluonteinen tieto päätyä vääriin käsiin, koska poistettu tieto on mahdollista palauttaa ilmaisohjelmien avulla.

ISO/IEC 27001-standardin mukaan tärkeimpiä tietoaineiston turvallisuudessa huomioitavia ja dokumentoitavia asioita on lueteltu taulukossa 10.

TAULUKKO 10 Tietoaineiston turvallisuudessa huomioitavia ja dokumentoitavia asioita (ISO/IEC 27001:fi 2006, 34) (Laakso Matti 2010, 43)

Aihe	Selite
Tietoaineiston inventaario	Määritellään suojeltavat kohteet sekä dokumentoidaan ne ja luokitellaan tärkeyden mukaan järjestykseen.
Omistaja	Määritellään jokaiselle kohteelle omistaja, jonka tehtävä on vastata tiedon suojaamisesta ja käsittelystä.
Tiedon salaaminen	Dokumentoidaan käytännöt ja periaatteet joilla tallennettavat tai käsiteltävät tiedot salataan.
Ohjeistaminen	Tietojen luokitteluun, käsittelyyn, tallentamiseen ja tuhoamiseen laaditaan ohjeet.

7.3.6 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudeksi kutsutaan kaikkia niitä keinoja, joilla suojataan dataverkoissa liikkuvan tiedon eheys, luottamuksellisuus ja saatavuus.

Sääilmiöt ovat yksi todennäköinen uhka tietoliikenneturvallisuudelle. Esimerkiksi ukkonen saattaa rikkoa yhdellä rysäyksellä puhelinkeskuksen, kaapeliverkko-osuuden tai matkapuhelimen.

Tietoturvaperiaatteisiin ja – käytäntöihin on järkevää dokumentoida tietoliikenneturvallisuuden suojamekanismit. Verkon ja laitteiden dokumentointi auttaa vikatilanteiden selvittelyssä ja ylläpidossa. Tietoliikenneturvallisuudelle on nimettävä myös vastuuhenkilöt.

Nykypäivän yrityksessä on käytössä erityyppisiä tietoverkkoja ja niiden käyttö lisääntyy koko ajan, joten mikäli yrityksellä ei ole asiantuntemusta tai kokemusta tietoliikenteen suojaamisesta niin sellaista kannattaa hankkia. Erilaisten tietoverkkojen turvallinen käyttö on hallittava. Älypuhelimien ja muiden vastaavien laitteiden lisääntyminen yrityksissä mahdollistaa tiedon sähköisen liikkumisen vaikka yrityksellä ei olisikaan omaa internet-yhteyttä. Näiden laitteiden tietoturva on yhtä tärkeää kuin perinteisten tietokoneiden.

Tietoliikenneturvallisuuteen liittyy myös verkkolaitteiden, kuten reitittimien, kytkimien ja palomuurien turvallisuus. Ensimmäinen toimenpide on estää verkkolaitteisiin liittyminen vierailta koneilta. Verkkolaitteiden avulla rakennetaan yrityksen tietoliikenneverkot, langalliset ja langattomat. Erityisesti langattomia tekniikoita käytettäessä on tärkeää ymmärtää niihin liittyvät riskitekijät, esimerkiksi tietomurron todennäköisyys, jos käytössä on vanhentunut salaustekniikka.

ISO/IEC 27001-standardin mukaan tärkeimpiä tietoliikenneturvallisuudessa huomioitavia ja dokumentoitavia asioita on lueteltu taulukossa 11.

TAULUKKO 11Tietoliikenneturvallisuudessa huomioitavia ja dokumentoitavia asioita (ISO/IEC 27001:fi 2006, 41–47) (Laakso Matti 2010, 42)

Aihe	Selite
Vastuuhenkilöt ja tehtävät	Nimetään vastuuhenkilöt ja vastuualueet tietoliikennettä koskeviin tehtäviin.
Tietoverkon rakenne	Tietoturvaratkaisut ja tietoliikenne verkot dokumentoidaan tarkasti. Verkkojen ylläpito on helpompaa, kun on laadittu hyvät dokumentit.
Tietoverkoissa liikkuvan datan suojaaminen	Tietoverkoissa liikkuvan datan suojauskeinot siirron aikana dokumentoidaan. Ohjeistus luodaan tarvittaessa.
Ohjeistaminen	Tietoliikenteen ylläpitäjiä ja peruskäyttäjiä varten on laadittava omat ohjeistuksensa. Henkilöstölle ohjeistetaan esimerkiksi yrityksen tietoverkon käytön periaatteet.
Sopimukset	Ongelmatilanteiden varalle verkon huolto- ja ylläpito- ja ulkoistamissopimukset on dokumentoitava tarkasti.

7.3.7 Henkilöstöturvallisuus

Henkilöstöturvallisuus on osa riskien hallintaa. Henkilöstön toimenkuviin tulee kuvata tietoturvavastuut ja tietoturvatehtävät riittävän selkeästi. Tärkeitä asioita ovat työhönottoon, toimenkuvan muutoksiin ja työsuhteen päättymiseen liittyvät toimenpiteet. Esimerkiksi uutta henkilöä rekrytoitaessa olisi hyvä tarkastaa henkilön tausta, sopivuus ja osaaminen. Liiketoiminnan kannalta tär-

keät avainhenkilöt pitäisi tunnistaa ja varmistaa heidän käytettävyytensä yrityksen palveluksessa. Suunnittelussa tulisi varautua lomiin, poissaoloihin, työnkiertoon ja väliaikaisjärjestelyihin riittävän hyvin sekä lisäksi valmentaa henkilöstö poikkeusoloihin. Työtyytyväisyys ja motivoitunut henkilökunta ovat tärkeä perusta tietoturvallisuuden toteutumiselle (Valtiovarainministeriö, 2007).

ISO/IEC 27001-standardin mukaan tärkeimpiä henkilöstöturvallisuudessa huomioitavia ja dokumentoitavia asioita on lueteltu taulukossa 12.

TAULUKKO 12 Henkilöstöturvallisuudessa huomioitavia ja dokumentoitavia asioita (ISO/IEC 27001:fi 2006, 36) (Laakso Matti 2010, 45)

Aihe	Selite
Vastuuhenkilöt ja vastuualueet	Määritellään henkilöstölle ja yhteistyökumppanille selkeästi omat vastuualueet ja varahenkilökäytännöt. Vaarallisten työyhdistelmien käyttöä on syytä välttää.
Tietoturvapolitiikka	Olennainen osa henkilöstön tietoturvallista työskentelyä on tietoturvapolitiikan hyväksyminen ja sen mukaan toimiminen.
Toimenpiteet työsuhteen alkaessa ja päättyessä.	Kuvaus toimenpiteistä, jotka suoritetaan kun yritykseen tulee uusi työntekijä tai yhteistyökumppani. Samaten kuvaus toimenpiteistä, jotka suoritetaan työntekijän tai yhteistyökumppanin erotessa.

Tietoturvakoulutus	Dokumentoidaan toimenpiteet, jotka on tehty tietoturvatietouden lisäämiseksi. Ilman soveltuvaa koulutusta, henkilöstön tietoturvallinen työskentely ei ole mahdollista.
Ulkoistaminen	Selvitetään ja dokumentoidaan muualta hankitun palvelun tietoturvallisuuden taso.

7.3.8 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan toimintaolosuhteita joilla yrityksen päivittäisten toimintojen ja rutiinien sekä tietotekniikan turvallinen käyttö ja ylläpito toteutetaan. Käyttöturvallisuuteen kuuluu esimerkiksi käyttöoikeuksien hallinta ja lokien valvonta. Varmuuskopiointi käytänteet ja haittaohjelmia vastaan suojautuminen ovat myös osa käyttöturvallisuutta. (Valtiovarainministeriö, 2007.)

8 KRIISIVIESTINTÄ

Ihmisiä, toimintaa tai mainetta uhkaavasta poikkeavasta tilanteesta tiedottaminen on kriisiviestintää. Tällaisessa tilanteessa nopea tiedonkulku on korvaamattoman tärkeää. Itse kriisi ei kaada yritystä, vaan se miten kriisi hoidetaan. Kriisitilanteen johtamisessa tärkeää on viestintä. Viranomaisilla ja tilannetta johtavalla toimijalla on aina tiedotusvastuu. On muistettava, että viestintä on yhteydenpitoa eri kohderyhmiin, henkilöstöön, asiakkaisiin, sidosryhmiin, kilpailijoihin ja päättäjiin. Kriisiviestinnän tulee olla nopeaa, selkeää, luotettavaa ja avointa. (Hakala Maija & Valkonen Noora, 2012.)

Kriisiviestinnän tavoitteena on:

- estää lisävahinkojen syntyminen
- ottaa kriisitilanne sisäisesti hallintaan
- tiedontarpeeseen reagointi
- turvallisuuden tunteen lisääminen.

(Hakala Maija & Valkonen Noora, 2012.)

Kriisitilanteen tapahduttua on ensimmäiseksi selvitettävä:

- mitä on tapahtunut, eli kriisin määrittäminen ja tilannekuvan rakentaminen.
- työnjako, kuka tekee ja mitä
- ensilausunnon anto
- tiedottaminen henkilöstölle, sidosryhmille ja asiakkaille.

(Hakala Maija & Valkonen Noora, 2012.)

Kriisitilanteen tilannekuvaa rakentaessa kannattaa selvittää vastaukset seuraaviin kysymyksiin:

- Mitä tiedetään varmasti? Mitä ei tiedetä?
- Mitä voi kertoa? Mitä ei voi kertoa?
- Mitä tehdään? Mitä ei saa tai voi tehdä?

(Hakala Maija & Valkonen Noora, 2012.)

Viranomaiset tiedottavat kriisitilanteen syistä, uhreista ja pelastustoimista. Yrityksen vastuulla on omaan toimintaansa liittyvä viestintä, vastuunkanto ja pahoittelut, riittävä tiedon tarjoaminen ja jatkotoimenpiteet. (Hakala Maija & Valkonen Noora, 2012.)

Normaaliaikana suunnitelmallisesti laaditut kriisiviestintäohjeet ja niiden harjoittelu ovat hyvä pohja onnistuneelle kriisiviestinnälle.

9 JATKUVUUS- JA TOIPUMISSUUNNITELMA

Jatkuvuus- ja toipumissuunnitelma laaditaan mahdollisten poikkeustilanteiden varalle, jotka riskienhallintasuunnitelma paljastaa. Niille suojeltaville kohteille, joiden riskin todennäköisyys ja vaikutus ovat suuret, laaditaan jatkuvuussuunnitelma. Jatkuvuussuunnitelma on kirjallinen ohjeistus toimenpiteistä miten yritys selviytyy erilaisista ongelma- ja poikkeustilanteista. Tällaisia tilanteita voivat olla esimerkiksi palvelintilan sähkökatko, vesivahinko tai murto. Mikäli tuotantolaitteiden eheydestä, luotettavuudesta tai saatavuudesta ei ole takuita, on yrityksellä oltava suunnitelma liiketoiminnan jatkuvuuden turvaamiseksi. (Tietoturvatietoa suomeksi, 2012d.)

Jatkuvuussuunnitelmassa yritys määrittää keinot, joilla poikkeustilanteisiin varaudutaan ja miten niistä selviydytään. Tärkeiden liiketoimintaprosessien palauttaminen normaalitasolle sekä riskien tiedostaminen ja hallinta ovat merkittävä osa tätä suunnitelmaa. Jatkuvuussuunnitelmaa kehitetään ja ylläpidetään koko ajan. Jotta suunnitelmasta tulisi mahdollisimman kattava, on sen laatimiseen osallistuttava kaikki yrityksen eri osastot, yritysjohdon lisäksi. (Tietoturvatietoa suomeksi, 2012d.)

Toipumissuunnitelmalla tarkoitetaan toimenpiteitä, joilla palautetaan yksittäisiä osia liiketoimintaprosesseista. Esimerkiksi sähköisissä toiminnanohjausjärjestelmissä, kaikkia asennettuja järjestelmiä, kuten laskutusta tai taloushallintoa varten tulisi olla oma toipumissuunnitelma. Toipumissuunnitelman pitäisi sisältää toimenpiteet järjestelmien palauttamiseksi toimintaan. Mikäli toipumissuunnitelma ja ohjeistukset ovat laadittu huolellisesti, pystytään toiminnanohjausjärjestelmä tai osia siitä palauttamaan toimintaan hyvinkin nopeasti ja luotettavasti. Toipumissuunnitelmia on kokeiltava myös käytännössä, jotta varmistutaan, että ne toimivat oikein. (Tietoturvatietoa suomeksi, 2012d.)

10 SUUNNITELMAN LAATIMINEN KESKI-SUOMEN KULJETUS OY:SSÄ

Projektin aloitus

Keski-Suomen Kuljetus Oy:ssä on aloitettu projekti riskienhallinnan ja liiketoiminnan jatkuvuudenhallinnan suunnitelman tekemiselle. Projekti toteutetaan yhdessä Huoltovarmuuskeskuksen kanssa. Keväällä 2012 suoritettiin projektin ensimmäinen vaihe, joka oli Huoltovarmuuskeskuksen laatima kypsyysanalyysi. Kypsyysanalyysin tarkoituksena oli selvittää, kuinka hyvin yritys on varautunut liiketoiminnan häiriötilanteisiin ja määritellä mikä on liiketoiminnan kannalta järkevä tavoitetaso. Kypsyysanalyysissä käsiteltiin kuutta liiketoiminnalle tärkeää osa-aluetta:

1. Jatkuvuudenhallinnan johtaminen
2. Jatkuvuudenhallinnan suunnittelu ja strategiat
3. Henkilöstön tehtävät jatkuvuudenhallinnan kehittämisessä
4. Kumppanuuksien ja resurssien jatkuvuudenhallinta
5. Toimintojen jatkuvuudenhallinta
6. Jatkuvuudenhallinnan kehittämisen mittarit

Kypsyysanalyysin tulokset ovat luottamuksellista tietoa, joten tässä työssä niitä ei käsitellä sen tarkemmin.

Suojeltavien kohteiden määrittely

Keski-Suomen Kuljetus Oy:ssä suojeltaviksi kohteiksi määriteltiin, Huoltovarmuuskeskuksen ohjeistuksen mukaisesti, rahtikuljetukset, urakointi, maa- ja kiviaineskauppa sekä kuljetukset, hallinto ja tietojärjestelmät. Jokainen suojeltava kohde jaettiin osa-alueisiin joita olivat, johtaminen, henkilöstö, toimitilat, toiminta ja yhteistyökumppanit.

Riskikartoitus

Riskikartoitus suoritettiin Huoltovarmuuskeskuksen laatiman ohjeen mukaan, luvussa 4 kerrotulla tavalla. Tulokset ovat luottamuksellisia, joten tässä työssä niitä ei käsitellä sen tarkemmin.

Tietoturva periaatteet ja käytänteet

Keski-Suomen Kuljetus Oy:ssä tietojärjestelmät oli yksi osa-alue riskikartoituksessa. Riskikartoituksen apuna käytettiin Pk-yrityksen riskienhallinnan verkkosivuilta löytyvää kysymyslistaa. Kysymykset olivat jaettu seuraaviin aihealueisiin

- Henkilöstön tietoisuus ja toimintatavat tietoriskien hallinnassa
- Tietojärjestelmien suojaus
- Tietoriskien hallinnan johtaminen ja organisointi
- Tietoriskit liike- ja sidosryhmäsuhteissa
- Toimintaympäristön sekä työ- ja palvelutilojen tietoturvallisuus.

Arviointiasteikko oli kolmeportainen; kyllä = asia on kunnossa, ei = asia täytyy selvittää ja ei koske meitä. (Pk-yrityksen riskienhallinta 2009a.)

Tietojärjestelmien suojausta koskevista kysymyksistä on muutama esimerkki kuviossa 5. Yksittäiset vastaukset ovat luottamuksellisia, joten niitä ei tässä työssä käsitellä.

Tietojärjestelmien suojaus

Tarkistuslista tietojen ja järjestelmien teknisten suojakeinojen kehittämiseen.

Yritys:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa yrityksen toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

Tietojen ja järjestelmien käyttöperiaatteet

	Kyllä	Ei	Ei koske meitä
Onko järjestelmien käyttöoikeuksien hallintaan nimetty vastuuhenkilö?	☐	☐	☐
Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?	☐	☐	☐
Ovatko pelisäännöt ja käytännöt työnantajalle kuuluvan sähköpostin lukemisesta poikkeustilanteissa sovittu yhdessä henkilöstön kanssa?	☐	☐	☐
Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilökohtainen salasana?	☐	☐	☐
Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?	☐	☐	☐
Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?	☐	☐	☐
Onko luottamuksellisten tietojen hävittämiselle silppurit tai lukitut paperisäiliöt?	☐	☐	☐
Onko tietojen siirto levykkeillä, CD:llä ja muilla tietovälineillä hallittua ja suojattua?	☐	☐	☐
Ovatko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin mahdollisen varkausvakuutuksen korvausta varten?	☐	☐	☐
Onko turvalliset etätyötavat ohjeistettu?	☐	☐	☐

KUVIO 5 Esimerkkikysymyksiä tietojärjestelmien suojauksesta. (Pk-yrityksen riskienhallinta 2009b)

Riskikartoituksen jälkeen tehtiin mm. seuraavia toimenpiteitä:

- Yhteistyökumppaneiden kanssa käytiin läpi sopimuksien sisällöt ja päivitettiin sopimukset vastaamaan nykyhetken tarpeita.
- Henkilöstölle järjestettiin koulutusta sähköisten järjestelmien tehokkaampaan käyttöön.
- Henkilöstöä ohjeistettiin siirrettävien tallennusvälineiden, kuten muistitikkujen ja cd/dvd-levyjen turvallisesta säilyttämisestä.

- Henkilöstöä ohjeistettiin älypuhelimien turvallisuusasioissa. Älypuhelimet ovat verkon päätelaitteita siinä missä kannettavat tietokoneetkin ja esimerkiksi sähköpostiviestit ohjautuvat näihin laitteisiin, siksi on tärkeää ymmärtää että yrityksen tärkeitä tietoja voi joutua vääriin käsiin puhelimen huolimattomasta käsittelystä johtuen.

Kriisiviestintäohje

Kriisiviestintäohje laadittiin Huoltovarmuuskeskuksen järjestämän koulutuksen ja ohjeistuksen pohjalta. Kriisiviestintäohjeeseen kirjattiin toimintaohjeet kriisitilanteen varalle, esimerkiksi miten ja kenelle kriisitilanteesta tiedotetaan ensimmäiseksi ja kuka yrityksessä vastaa tiedottamisesta julkisuuteen.

Jatkuvuus- ja toipumissuunnitelma

Riskikartoituksen tuloksien perusteella laadittiin Keski-Suomen Kuljetus Oy:lle jatkuvuus- ja toipumissuunnitelma mahdollisten poikkeustilanteiden varalle. Suunnitelma sisältää mm.

- suurimmille uhkille tehtävät korjaavat toimenpiteet ja aikataulun
- vastuuhenkilöt
- toimintaohjeistuksen kriisitilanteessa
- seuraavan riskikartoituksen ajankohdan.

11 LOPPUSANAT

Opinnäytetyöni tarkoitus oli laatia liiketoiminnan riskienhallinnan ja jatkuvuuden hallinnan suunnitelma Keski-Suomen Kuljetus Oy:lle. Aiheeseen liittyvää lähdemateriaalia oli saatavilla valtavan paljon ja haasteeksi syntyikin työn rajaaminen sopivan kokoiseksi. Opinnäytetyön alkuosa käsittelee aihetta yleisellä tasolla ja sitä kirjoittaessani oma tietoisuuteni aiheesta lisääntyi merkittävästi. Työn loppuosassa kerron niitä toimenpiteitä joita Keski-Suomen Kuljetus Oy:ssä tehtiin suunnitelman laatimiseksi.

Erilaisten tietojärjestelmien ja sähköisten järjestelmien lisääntymin yritysmaailmassa tuo haasteita myös tietoturvallisuuteen ja sen ymmärtämiseen. Tämän takia myös Keski-Suomen Kuljetus Oy:lle laadittiin tietoturvaperiaatteet ja käytänteet. Tavoitteena oli luoda yksinkertainen ja selkeä ohjeistus tietoturvallisuuteen. Mielestäni saavutin tämän tavoitteen.

Opinnäytetyön tuloksena laaditut riskienhallintasuunnitelma, jatkuvuus- ja toipumissuunnitelma sekä tietoturvaperiaatteet ja – käytänteet tullaan kirjoittamaan osaksi Keski-Suomen Kuljetus Oy:n laatujärjestelmää. Suunnitelmia päivitetään ja pidetään yllä vuosittain.

Keski-Suomen Kuljetus Oy:n henkilökunta oli ansiokkaasti mukana laatimassa riskikartoituksia ja suunnitelmia. Heidän ammattitaidostaan oli suuri apu eri liiketoimintayksiköiden riskikartoituksissa ja oma tietämykseni lisääntyi paljon koko yrityksen toiminnasta.

Lähteet

Finlex. 2004. Edita Publishing Oy. Sähköisen viestinnän tietosuojalaki 16.6.2004/516. Viitattu 15.7.2012. http://www.finlex.fi/fi/laki/ajantasa/2004/20040516?search[type]=pika&search[pka]=S%C3%A4hk%C3%B6isen%20viestinn%C3%A4n%20tietosuojalaki%2016.6.2004%2F516

Hakala, M., Vainio, M & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Hakala, M., Valkonen, N. 2012. Viestintä tilannejohtamisen työvälineenä. Luentomateriaali. Kriisiviestintäkoulutus Ähtärissä 13.9.2012.

Huoltovarmuuskeskus. 2012. Jatkuvuudenhallinta. Viitattu 12.6.2012. www.huoltovarmuus.fi.

ISO/IEC 27001:fi. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing Oy.

Laakso, M. 2010. PK-Yrityksen tietoturvasuunnitelman laatiminen. Opinnäytetyö. Turun ammattikorkeakoulu. Tietojenkäsittely, Tietoliikenne. Viitattu 2.12.2012. http://publications.theseus.fi/bitstream/handle/10024/20793/laakso_matti.pdf?sequence=1

Maakuljetuspooli. 2012. Systemaattinen riskianalyysi liiketoiminnan tukena. Luentomateriaali. Riskienhallintakoulutus Keuruulla 9.5.2012.

Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen. Näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Talentum Media Oy.

Mäkinen, R. 2003. Tietoturvapolitiikat. Helsinki. Helsingin yliopisto. Tietojenkäsittelytieteen laitos. Viitattu 5.12.2012. http://www.cs.helsinki.fi/group/turvasem/abstracts/tietoturvapolitiikat_ea.pdf

Pk-yrityksen riskienhallinta 2009a. Tietoriskit. Viitattu 15.10.2012. http://www.pk-rh.com/riskilajit/tietoriskit/tietoriskit.html.

Pk-yrityksen riskienhallinta 2009b. Tietoriskit. Viitattu 15.10.2012. http://www.pk-rh.com/pdf/tietojarjestelmien-suojaus.pdf

Raggad, B. G. 2010. Information Security Management. Concepts and Practice. Boca Raton: CRC Press.

Rosqvist, T., Tuominen, R., & Sarsama, J. 2006. Huoltovarmuuden turvaamiseen tähtäävä logistisen järjestelmän riskianalyysimenetelmä. VTT Publications. Viitattu 5.12.2012. http://www.vtt.fi/inf/pdf/publications/2006/P602.pdf

Tietoturvatietoa suomeksi 2012a. Viitattu 15.8.2012. http://www.tietojesiturvaksi.fi/content/tietoturvallisuuden-perusk%C3%A4sitteit%C3%A4

Tietoturvatietoa suomeksi 2012b. Viitattu 15.8.2012. http://www.tietojesiturvaksi.fi/content/lains%C3%A4%C3%A4d%C3%A4nn%C3%B6n-vaikutukset.

Tietoturvatietoa suomeksi 2012c. Viitattu 15.8.2012. http://www.tietojesiturvaksi.fi/content/tietoturvan-osa-alueet.

Tietoturvatietoa suomeksi 2012d. Viitattu 15.8.2012. http://www.tietojesiturvaksi.fi/content/jatkuvuus-ja-toipumissuunnitelma.

Valtionvarainministeriö 2007. Tietoturvallisuudella tuloksia 3/2007. Viitattu 15.11.2012. https://www.vahtiohje.fi/web/guest/kayttoturvallisuus.

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia 3/2007. Viitattu 15.11.2012. https://www.vahtiohje.fi/web/guest/henkilostoturvallisuus.

Valtiovarainministeriö 2012. Tietoturvallisuus. Viitattu 15.7.2012 http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp